Claims:

What is claimed is:

1. A method for protecting public key schemes from timing, power monitoring and fault attacks comprising the steps of:

obtaining a message for use in a crypotographic operation;

obtaining a modulus and an exponent corresponding to said crypotographic operation, wherein said exponent contains at least one bit;

initializing a first value as a one, and assigning said message to a second value;

executing a modulo exponentiation algorithm on each bit of said exponent from the most significant bit to the least significant bit, wherein said algorithm comprising the steps of:

input a bit to an inverter and storing the output as a third value, and assigning the next bit of said bit as a fourth bit;

if said third value is a zero, updating said first value with the result of squaring, modulo said modulus said first value, if said third value is a one, updating said first value with the result of multiplying, modulo said modulus said first value by said second value; and

if said fourth value is a zero, updating said first value with the result of squaring, modulo said modulus said first value, if said fourth value is a one, updating said first value with the result of multiplying, modulo said modulus said first value by said second value;

updating said bit with the next bit of said bit, and executing steps of said algorithm on said bit until said bit being said least significant bit of said exponent; and

storing and output said first value.

2. A method according to claim 1, wherein if said bit is said least significant bit of said exponent, said fourth value is initialized as 1.

3. A method according to claim 2, wherein said bit is one bit of bits of said exponent and is a one or a zero.

4. A method according to claim 1, wherein said inverter is used for output a one if input a zero into it, and output a zero if input a one into it.

5. An apparatus for protecting public key schemes from timing, power monitoring and fault attacks comprising:

means for obtaining a message for use in a crypotographic operation;

means for obtaining a modulus and an exponent corresponding to said crypotographic operation, wherein said exponent contains at least one bit;

means for initializing a first value as a one, and assigning said message to a second value;

means for executing a modulo exponentiation algorithm on each bit of said exponent from the most significant bit to the least significant bit, wherein said algorithm comprising:

means for input a bit into an inverter and storing the output as a third value, and assigning the next bit of said bit as a fourth bit;

means for determining whether said third value is a one or a zero;

means for updating said first value with the result of squaring if said third value is a one, modulo said modulus said first value, updating said first value with the result of multiplying, modulo said modulus said first value by said second value if said third value is a one;

means for determining whether said fourth value is a one or a zero; and

means for updating said first value with the result of squaring, modulo said modulus said first value if said fourth value is a zero, updating said first value with the result of multiplying, modulo said modulus said first value by said second value if said fourth value is a one;

means for updating said bit with the next bit of said bit, and executing steps of said algorithm on said bit until said bit being said least significant bit of said exponent;

means for determining whether said bit is a one or a zero; and

means for storing and output said first value.

6. An apparatus according to claim 5, wherein said bit is one bit of bits

of said exponent and is a one or a zero.

7. An apparatus according to claim 5, wherein said inverter is used for output a one if input a zero into it, and output a zero if input a one into it.

8. A computer-readable medium for protecting public key schemes from timing, power monitoring and fault attacks containing logic code that executing the steps of:

obtaining a message for use in a crypotographic operation;

obtaining a modulus and an exponent corresponding to said crypotographic operation, wherein said exponent contains at least one bit;

initializing a first value as a one, and assigning said message to a second value;

executing a modulo exponentiation algorithm on each bit of said exponent from the most significant bit to the least significant bit, wherein said algorithm comprising the steps of:

input a bit to an inverter and storing the output as a third value, and assigning the next bit of said bit as a fourth bit;

if said third value is a zero, updating said first value with the result of squaring, modulo said modulus said first value, if said third value is a one, updating said first value with the result of multiplying, modulo said modulus said first value by said second value; and

if said fourth value is a zero, updating said first value with the result of squaring, modulo said modulus said first value, if said fourth value is a one, updating said first value with the result of multiplying, modulo said modulus said first value by said second value;

updating said bit with the next bit of said bit, and executing steps of said algorithm on said bit until said bit being said least significant bit of said exponent; and

storing and output said first value.

9. A computer-readable medium according to claim 8, wherein if said bit is said least significant bit of said exponent, said fourth value is initialized as 1.

10. A computer-readable medium according to claim 9, wherein said inverter is used for output a one if input a zero into it, and output a zero if input a one into it.

11. A computer-readable medium according to claim 8, wherein said bit is one bit of bits of said exponent and is a one or a zero.